Intrusion Detection with Snort Part–II

On the Alert

This second part of the two-part article offers a step-by-step approach to put the Snort Network Intrusion Detection System (NIDS) into action.

Before proceeding further, the most important thing that one needs to do is to decide on where to place the Snort NIDS in the network. In general, Snort should be placed at a point in the network where it can see all the network traffic. If you use a firewall to protect your network, then placing Snort outside the firewall will help you to see all the external attacks that are coming to your network. Note that some of these attacks may not reach your internal network because of the filtering done by the firewall. On the other hand, placing Snort behind the firewall will help you to see all the internal attacks and also the ones that managed to cross the firewall from the outside.

Using Snort in a switched network may involve some additional configurations on the switch device. In a switched network, all switch ports do not see all the traffic. So it has to be explicitly configured to mirror all the traffic to the port on which Snort is connected. (Refer to the switch device manual to know more about mirroring.)

With this knowledge in place, let's move on to the steps involved in setting up Snort.

Step 1

Download the latest source version of Snort NIDS for your platform from www.snort.org

Step 2

Follow the steps given below to build and install Snort on your hard disk...

```
# tar zxf snort-<ver>.tar.gz
# cd snort-<ver>
# ./configure
# make all
# make install
```

Note: *Snort depends on the libpcap packet sniffing library to sniff packets from the network. You can get the libpcap library from http://www.tcpdump.org/*

The following steps to build and install libpcap...

```
# tar zxf libpcap-<ver>.tar.gz
# cd libpcap-<ver>
# ./configure
# make all
# make install
```

Step 3

Edit the Snort configuration file (<snort_install _dir>/etc/snort.conf) and specify your internal and external network address (HOME_NET & EXTERNAL_NET). You can use the default setting, *any*, to indicate any IP address.

Step 4

To reduce false positives, specify your server's IP address and port in the Snort configuration file. Table 1 shows the list of Snort variables that you may need to edit.

Step 5

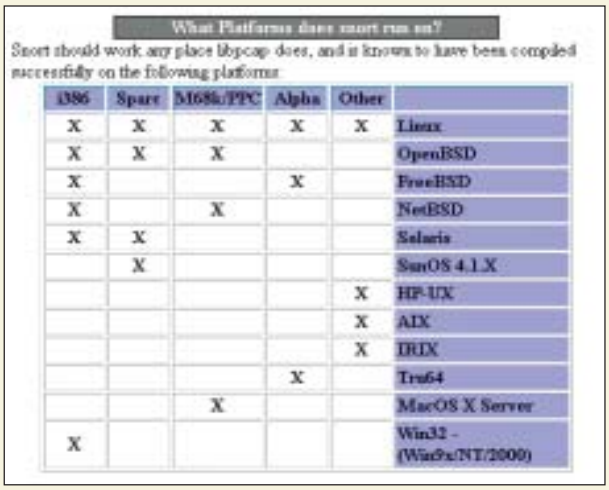
The next step is to configure output plug-ins. All that you may need to do is to uncomment the output plug-in that you want to use in the Snort configuration file. Table 2 lists the output plug-ins that are available in Snort 2.X.

You can also create a custom rule type that can

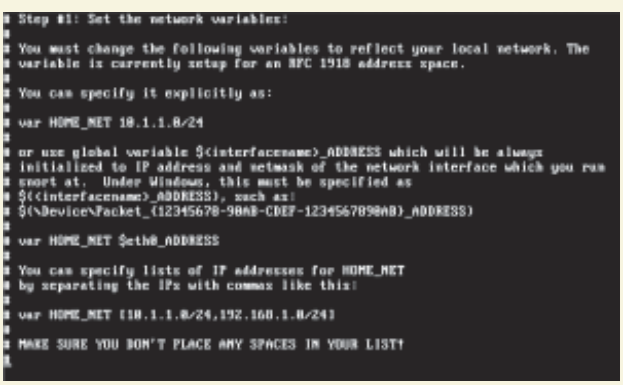
Table 1

Snort variable	Description
DNS_SERVERS	List of name resolution servers in your network
SMTP_SERVERS	List of e-mail servers in your network
HTTP_SERVERS	List of Web servers in your network
SQL_SERVERS	List of database servers in your network
TELNET_SERVERS	List of telnet servers in your network
SNMP_SERVER	List of SNMP servers in your network
HTTP_PORTS	List of Web server ports
SHELLCODE_PORTS	Ports you want to look for SHELLCODE
ORACLE_PORTS	Ports you want to look for Oracle attacks

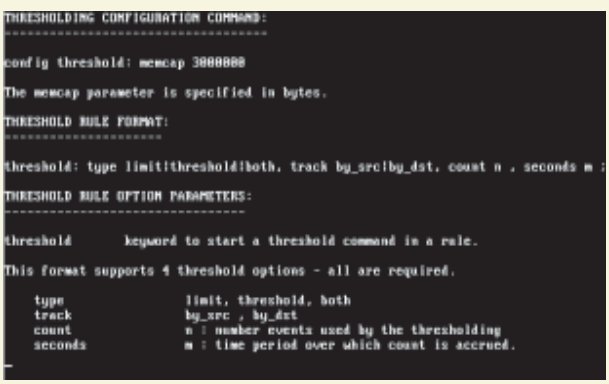
Snort's website



Snort runs on multiple platforms



Snort configuration file



Threshold settings

Table 2

Output plug-in module	Description
alert_syslog	Log alerts as SYSLOG messages. You can specify the SYSLOG facility and priority as arguments to this plug-in
log_tcpdump	Log packets in tcpdump format. You can specify the file name as argument to this plug-in
Database	Log alerts or packets to database. Refer to the Snort user manual for supported list of database.

use a combination of these output modules for alerting/logging. The following script shows a custom rule type that instructs Snort to log all the alerts as SYSLOG messages and also to a MYSQL database...

```
ruletype custom
{
type alert
output alert_syslog: LOG_AUTH
LOG_ALERT
output database: alert,
mssql,dbname=snort user=snort
password=test
}
```

Following example is a rule that uses the above custom rule type as the rule action...

```
custom tcp $HOME_NET any ->
$EXTERNAL_NET any
```

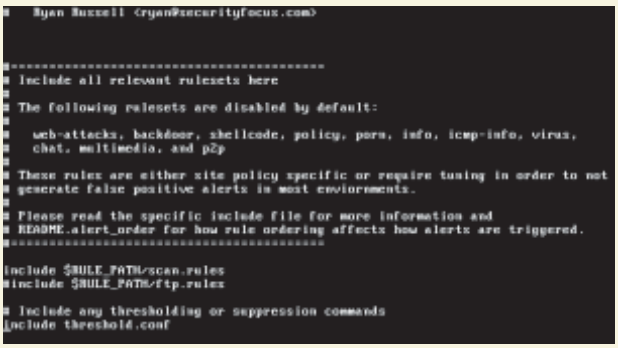
Step 6

If you want to either create a new custom alert classification and priorities or update the pre-defined ones, then edit <snort_install_dir>/etc/classification.config and add or update the classification entries. The following example shows a pre-defined alert classification defined in <snort_install_dir>/etc/classification.config and used in the <snort_install_dir>/rules/scan.rules

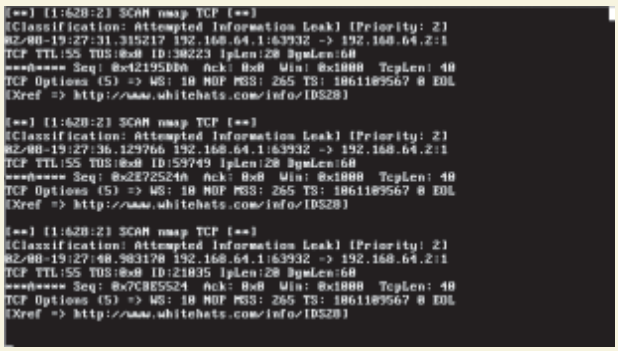
```
config classification: attempted-
recon,Attempted Information Leak,2

alert tcp $EXTERNAL_NET any ->
$HOME_NET any (msg:"SCAN nmap
TCP"; flags:A,12; ack:0;
reference:arachnids,28;
classtype:attempted-recon; sid:628;
rev:2;)

[**] [1:628:2] SCAN nmap TCP [**]
[Classification: Attempted Information
Leak] [Priority: 2]
02/09-10:18:57.732953
192.168.64.1:33777 -> 192.168.64.2:1
TCP TTL:43 TOS:0x0 ID:43390 IpLen:20
```



Select the desired rules



Snort in action

```
DgmLen:60
***A**** Seq: 0x4BC7EAFB  Ack: 0x0
Win: 0x1000  TcpLen: 40
TCP Options (5) => WS: 10 NOP MSS:
265 TS: 1061109567 0 EOL
[Xref => http://www.whitehats.com/
info/IDS28]
```

Step 7

If you want to either create a new alert reference or update the pre-defined one, then edit <snort_install_dir>/etc/reference.config. The following example shows a pre-defined alert reference defined in <snort_install_dir>/etc/reference.config and used in the <snort_install_dir>/rules/scan.rules

config reference: arachnids http://www.whitehats.com/info/IDS

```
alert tcp $EXTERNAL_NET any ->
$HOME_NET any (msg:"SCAN nmap
TCP"; flags:A,12; ack:0;
reference:arachnids,28;
classtype:attempted-recon; sid:628;
rev:2;)
```

```
[**] [1:628:2] SCAN nmap TCP [**]
[Classification: Attempted Information
Leak] [Priority: 2]
02/09-10:18:57.732953
192.168.64.1:33777 -> 192.168.64.2:1
TCP TTL:43 TOS:0x0 ID:43390 IpLen:20
DgmLen:60
***A**** Seq: 0x4BC7EAFB  Ack: 0x0
Win: 0x1000  TcpLen: 40
TCP Options (5) => WS: 10 NOP MSS:
265 TS: 1061109567 0 EOL
[Xref => http://www.whitehats.com/
info/IDS28]
```

Table 3

Threshold type	Description
Limit	Alert on the first event during the specified time interval and ignore the rest of the events
Threshold	Alert every time when the number of events crosses the specified threshold limit during specified time interval
Both	Combination of limit and threshold

Step 8

Configure threshold settings in <snort_install_dir>/etc/threshold.conf. You may need to do this if you want to reduce the number of alerts generated by Snort. Currently Snort supports three types of thresholds (shown in Table 3).

Step 9

Enable or disable the required rule sets and rules based on your network requirements.

Step 10

Run Snort in NIDS mode...

```
# snort –N –q –l <log_dir> -c
<snort_install_dir>/etc/snort.conf -D
```

Step 11

Snort in action: Viewing Snort alerts.

And this is all that's required to put Snort into action. LFY

By: Raja R.K.The author is a lead engineer working in HCL Technologies (Cisco Systems Offshore Development Centre) in Chennai. He has more than five years of experience in software development including two years in Linux. He holds a B.E. degree in computer science & engineering from S.R.M Engineering College. He can be contacted at rajark_hcl@yahoo.co.in